REMARKS

Claim 33 has been added. Claims 1-33 are pending.

In the Office action, the claims were rejected as follows:

(1) Claims 1-8, 12-15, 17-22 and 24-29 are rejected as obvious from the combination of U.S. Patent No. 5,737,418 (Saffari et al.) and either U.S. Patent No. 6,186,339 (Saltsov et al.) or U.S. Patent No. 6,223,876 (Walsh et al.).

(2) Claims 9-11, 16, 23 and 30-32 are rejected as obvious from those references in view of U.S. Patent No. 5,933,816 (Zennah et al.).

As discussed below, applicant respectfully requests reconsideration.

The primary reference cited by the Office action is the Saffari et al. patent, which discloses techniques for encrypting bill validation data generated by a bill validator, sending the encrypted data to gaming or vending machine, and decrypting the data to obtain the original bill validation data. The encryption key may be changed for subsequent transmissions of data by selecting a new key word from a key table that is maintained by both the validator and the gaming or vending machine. Following decryption, the gaming or vending machine evaluates a checksum that was transmitted with the bill validator data to check the integrity of the received data.

As explained below, the pending claims are patentable over the cited references.

In particular, the Office action appears to confuse authenticating a banknote or bill with authenticating a message or data from the bill validator. Authenticating a banknote or bill involves determining whether the banknote or bill is genuine. In contrast, authenticating a message from the bill validator involves determining whether the message is from an authorized source. As explained according to one scenario in the Background section of the pending Specification:

> Since a transaction message sent by a bill acceptor over the communications channel may not be secure, an unauthorized person with this knowledge may be

able to replace the bill acceptor with an unauthorized bill acceptor. Then the unauthorized bill acceptor could be programmed to replicate a transaction message that would have been sent by the original, legitimate bill acceptor. Since the transaction controller lacks a mechanism for determining the validity of the transaction message, the unauthorized bill acceptor unit is able to convince the transaction controller that it is the authorized bill acceptor. Thus, the transaction controller is duped into generating a credit based on a fraudulent transaction, thus permitting a thief to steal a good or service. The currency-handling machine thus has no mechanism for authenticating the source of the transaction message and determining whether a transaction message originated from the original authorized bill acceptor.

The Office action also appears to confuse the idea of authenticating a message (*i.e.*, determining whether the message is from a legitimate source, for example, by evaluating a key extracted from the message) and the idea of checking the integrity or validity of a message to ensure that data in the message has not become corrupted during transmission (*e.g.*, such as by evaluating a checksum).

For example, claims 1 and 24 recite "enabling the bill acceptor to accept a bill *if the decrypted transaction message is authenticated.*" Although the Saffari et al. patent discloses validating a bill and encrypting/decrypting bill validator data, there is no suggestion of authenticating the message, as recited in claims 1 and 21.

As noted above, the Saffari et al. patent does mention evaluating a checksum that was transmitted with the bill validator data to check the integrity of the received data. However, as explained by the Saffari et al. patent, evaluating the checksum only helps ensure that the received bill validator data was not corrupted during transmission (col. 6, lines 55-57). It says nothing about whether the message is authenticated (*i.e.*, whether it is from an authorized bill validator).

According to the Saffari et al. patent, a bill determined by the validator to be valid may still be rejected by the machine (*e.g.*, if the machine determines that the bill's denomination or country of origin is unacceptable). However, such a determination does not relate to the authenticity of the message and does not indicate that the message came from an illegitimate source.

The Walsh et al. and Saltsov et al. patents disclose, respectively, authenticating banknotes and evaluating properties of paper currency. However, as already noted, determining that a banknote authentic (*i.e.*, genuine) is very different from authenticating a message from a bill validator.

The Zennah et al. patent also does not disclose or suggest the features missing from the other references.

At least for those reasons, claims 1 and 24, as well as dependent claims 2-11 and 25-33, should be allowed.

Claims 17 and 19 recite verifying the "authenticity" of an encrypted transaction message. As discussed above in connection with claims 1 and 24, the Saffari et al. patent does not disclose or suggest checking the authenticity of the message. Instead, it only discloses using encryption to make it more difficult for someone to reverse engineer the system for encoding bill validation data (col. 2, lines 5-8). As also explained, checking the integrity of the received data by evaluating the checksum is significantly different from authenticating the message.

At least for those reasons, claims 17 and 19, as well as dependent claims 18 and 20, should be allowed. For similar reasons, claims 21-23 should be allowed.

The subject matter of pending claim 12 can be used, for example, as part of set-up mode and includes transmitting a certificate key from the transaction controller (*e.g.*, in the vending machine) to the bill acceptor to enable the bill acceptor to operate. There is no disclosure or suggestion in the Saffari et al. patent of sending any key from the gaming or vending machine to the bill acceptor. Instead, the bill acceptor and the machine use the same encryption key because

they both store the same key table (col. 12, lines 22-24). In some cases, the validator and the machine may need to resynchronize to ensure that they will use the same encryption key (col. 11, lines 3-35). However, that does not involve sending an encryption key from the machine to the bill validator (or vice-versa).

The other cited references also do not disclose or suggest those features.

At least for those reasons, claim 12 should be allowed.

Claim 13 includes a feature that allows a *new* certification key to be used. When a (stack or credit) command is sent to the bill acceptor (*e.g.*, from the transaction controller), the command also includes a new certification key that may be used to authenticate the *next* message.

As mentioned above, the Saffari et al. patent discloses a technique for changing the encryption key, but the technique for doing so does not involve sending a new key certificate to the bill validator.

Instead, according to the Saffari et al. patent, both the bill validator and the gaming or vending machine execute the same algorithm using three independent sources of information (raw validation data, the encryption key, and the number of bills accepted since the last synchronization) to calculate a value that subsequently is used to move pointers to a new key word in the tables stored by both the validator and the machine (col. 7, lines 18-21; col. 9, line 51 – col. 10, line 23; col. 12, lines 36-45).

The other references do not disclose or suggest the features missing from the Saffari et al. patent.

At least for those reasons, claim 13, as well as claim 14, should be allowed.

Claims 15 and 16 also mention a certificate key. Such certificate keys, which are used for authentication purposes, are different from the encryption keys disclosed in the Saffari et al. patent. Furthermore, each of those claims refers to several different types of keys. For example, claim 15 recites "retrieving the certificate key and the master key." Similarly, claim 16 refers to

a certificate key, as well as a public key and a private key. There is no disclosure or suggestion in the Saffari et al. patent of different types of keys. Although the Zennah et al. patent mentions a "public key certificate," that disclosure is in the context of authenticating a customer (col. 16, lines 42-45). There is no suggestion of that such a certificate could be used in the context of transmissions between a bill validator and a gaming or vending machine. Nor is there is any suggestion of how such a certificate might be used in the context of bill validators. A contrary conclusion would be precisely the type of improper hindsight the Court of Appeals for the Federal Circuit has warned against.

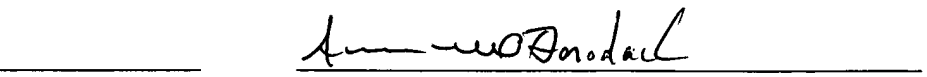
At least for those reasons, claims 15 and 16 should be allowed.

Claims 22 and 23, which depend from claim 21, also recite the use of certification keys. In addition to the reasons discussed above with respect to claim, claims 22 and 23 should be allowed for the additional reasons discussed with respect to claims 15 and 16.

Enclosed is a check for excess claim fees. Please apply any other charges or credits to deposit account 06-1050.

Respectfully submitted,

Date: 1/10/05



Samuel Borodach
Reg. No. 38,388

Fish & Richardson P.C.
Citigroup Center
52nd Floor
153 East 53rd Street
New York, New York 10022-4611
Telephone: (212) 765-5070
Facsimile: (212) 258-2291